COVER SHEET

Future Standardization Areas for Identity Management Systems

Suriadi Suriadi[1], Paul Ashley[2] and Audun Jøsang[1]

[1] Information Security Institute
Queensland University of Technology
Brisbane QLD 4000 Australia
s.suriadi@isi.qut.edu.au, a.josang@qut.edu.au

[2] IBM Software Group
Australia Development Laboratory
Southport QLD 4215 Australia
pashley@au1.ibm.com

Abstract. There are several areas of identity management that require standardization in order for them to work effectively. This paper proposes three standardization areas: the development of fine-grained privacy standards, the negotiation standards, and the backward privacy standards. Backward privacy refers to the problems that arise due to the massive amount of the already revealed personal information in the past which might reduce, or render useless, the effectiveness of the use of the privacy enhancing identity management system in the future. The main characteristics that each standard should have are also laid out in this paper.

1 Introduction

The development of a privacy enhancing identity management system has received some substantial attention recently. The solution proposed by the PRIME project [3][6] marks a significant advancement toward this end. However, several areas in the identity management area, not limited to PRIME, need some standardization efforts for them to function effectively. In this paper, the term 'standards' is used loosely to mean a set of standardized guidelines that businesses should follow, instead of the more common technical connotation of the term.

We will propose three areas in which the standardization efforts would help in ensuring a successful implementation of a privacy enhancing identity management system. The first one is the need for privacy standards, as has been mentioned by Borking [2], but this paper will argue for its need from the users' usability point of view and the need to have a more fine-grained privacy standardization.

The second potential standardization area is in the negotiation process. Several approaches that PRIME uses, such as the use of trust and privacy policy

negotiations, require further standardization in order for them to function effectively. We argue that without a framework to guide the proper implementation of the the negotiation process, this scheme, while potentially useful, could also be a tool that jeopardizes users' privacy.

Finally, while privacy enhancing identity management systems are useful to protect one's privacy, in reality, it might be too late unless some efforts are concentrated on securing the information of millions of users that has already been known to various organizations. This problem is especially relevant for static personal information like date of birth, social security number, tax file number, and so on. There should be some agreement on how to deal with this problem, for otherwise, the use of privacy enhancing identity system will not do much to reclaim one's privacy.

This paper will argue the importance of these three issues and how standardization will help in making these situations at least manageable.

2 Privacy Standards for Usability

In the paper by Borking [2], the need for privacy standards were argued from the business perspective. The benefits of having global privacy standards, as argued in this paper, include the reduction of privacy compliance cost on a global scale, reduction in the risk of developing new technologies, and several others.

In addition to those benefits, having privacy standards will also be useful from the users' usability point of view. The current practice of providing a lengthy explanation of a company's privacy statement is not usable from the users' perspective. In particular, it violates the *security usability* principal as proposed by Josang et al [5]: it is unreasonable to expect the users to have to read this lengthy explanation repeatedly in order to draw a conclusion about the privacy policy. Besides, the mental load required of the users to do such an action repeatedly is also intolerable.

With the existence of privacy standards, a service provider can simply provide a statement about the level of their privacy practice compliance with the standards. Of course this means that the privacy standards need to have a set of evaluation criteria to categorize a company's privacy policy to a list of compliance level. A succinct description of what this compliance level means to a user is a more usable approach. The enforcement of the claimed privacy compliance level is another important problem that needs to be addressed, but it is beyond the intended scope of this paper. Users that are truly concerned about their privacy could refer to the original privacy standards document, preferably the summarized version if one exists, and read what a compliance level means, and this should only be done once, hence it is still tolerable from the security usability principle point of view.

Therefore, we argue that the need of privacy standards is even more important, not only from the business perspective, but also from the users' usability perspective. In addition, having privacy standards will also make the standard-

ization efforts of the other areas of identity management easier, as will be explained in section 3 and 4.

2.1 Characteristics of Privacy Standards

There are several existing privacy legislations, including those that apply across various countries, such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [3]. However, one of the problems with such legislations is that they can only be applied to OECD nations, and it still leaves the harmonization of the legislation with other countries' privacy legislations problematic. Another problem is that while these could very well be a good legislations, more fine grained privacy standards are needed, especially in order to specify how the users' information will be treated at the service providers side, according to the privacy level compliance. Therefore, privacy standards that are aimed at a global scale should consider the following:

- **Privacy Areas**: the existing privacy legislations should be broken down into several key privacy areas as the basic framework for the privacy standards [2]. For example, these privacy areas could be on the limit on the use of personal information, data sharing, treatment of the personal information stored, and so on.
- **Fine Grain Privacy Specification**: the privacy standards should be at a reasonable fine-grained level that specifies exactly how a piece of personal information will be treated, as per the privacy level compliance at each area of the privacy standards. For example, in the area of data sharing, the more fine-grained privacy standards could be:
  - Level 1 Privacy: Users' personal information will be shared to related companies unless explicit request by the user to opt out from such a practice is given.
  - Level 2 Privacy: Users' personal information will not be shared to related companies unless explicit consent from the user is obtained.
  - Level 3 Privacy: Users' personal information will not be shared to related companies, unless explicit consent from the user is obtained that indicates precisely what information to share and to which company the information is to be shared.
  - Level 4 Privacy: Users' personal information will not be shared to any companies for whatever reasons.
- **Input from Users and Businesses**: the privacy standards should consider both the requirements from the users and the businesses to ensure that the adoption of the standards a success.
- **Conformance Guidelines**: there should be a guidelines to determine the classification of a company's privacy practice into the standards conformance level.

[3] `http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html`

3 Negotiation Standards

PRIME introduces the concept of trust and privacy policy negotiations between users and providers prior to releasing any personal data. While it is a good concept, in practice, there are several issues that require some standardization efforts to avoid unwanted situations, especially given that up to this point, the concept of negotiation on the release of personal information has not been widely practiced in an online environment.

3.1 Balance and Fair Negotiation Practice to Avoid Abuse

In a traditional on-line environment, when a service provider requires some information about a user, the user can either provide the correct information or lie about them. In this situation, a service provider can only make sure that certain fields are filled in a specific format, but the assertion that the information is correct is not stressed upon.

Abuse of the negotiation system could be done when there are unfair and unregulated negotiation practices whereby the service providers have most of the negotiation power and demand unreasonable users' information, and worse, persistently require certified information about the users' information. A poorly executed negotiation procedure without any balance of power between the service providers and the users will only aggravate the lack of users' control over their personal information. A potential manifestation of this problem is to have the service providers to demand the users to either provide the information or be refused services, in which case, the users will most likely sacrifice their privacy demands.

Similarly, it is just as undesirable in a completely overturned situation whereby the users have more power than the service providers, though seemed to be unlikely. While privacy is important, there is also a need for proper accountability practice to handle exceptional circumstances. When the users have more power, they might prefer to be completely anonymous and thus making accountability process impossible.

Therefore, a balanced and fair negotiation procedure should be standardized. Without this standards, each service provider will implement their own negotiation procedure that they deemed acceptable from their point of view, which might result in an imbalance outcome. There is a fine line between having more information about a user than needed and not having enough information for a proper accountability investigation. This has to be regulated in the form of a standardized negotiation practice. The aim of this standardized negotiation procedure is to provide an acceptable common negotiation practices that are acceptable to both the businesses and the users that will result in a common agreement to proceed with the intended transaction(s). More importantly, the standard should be designed in a balanced and fair manner to both users and business organizations. Ideally, the negotiation practice should be reflected according to the privacy level (as mentioned in 2) that an organization complies to.

3.2 Negotiation Deadlock

In any negotiation process, it is not unlikely that an agreement cannot be reached between the negotiating parties. For example, a service provider might want the user to provide the actual value of their date of birth, while the user is only willing to state that they are above a certain age in their privacy policy preference. This will result in a negotiation deadlock and most likely, the user will then be refused services.

Relating to the need for a balance and fair negotiation practice, it is therefore important that a standardization effort is done to handle this situation. In particular, the standards should should provide some clear guidelines on to handle such a negotiation deadlock situation without, ideally, causing refusal of service to the users.

3.3 Negotiation Subjects

Another aspects to look at in the negotiation process is the subject of the negotiation itself. PRIME proposes the trust and policy negotiations (see section 3.5 of [7]). However, we would argue that there are two other negotiation subjects that would provide a better negotiation process: the personal information to be released and the disclosure level of the information.

Personal information negotiation refers to the type of data to be released, such as the date of birth, address, nationality, financial information, and so on. The disclosure level refers to whether the exact value of the data is to be revealed or simply releasing the characteristics of the data. For example, instead of disclosing exact address, a statement that a user lives in a particular suburb or a state is given. An example of such a model was proposed by Williams and Barker in [8].

The combination of trust, privacy policy, the type of data to be released and the level of disclosure of the data should provide a flexible negotiation space for the parties to reach an agreement. The challenge is, however, the complexity of the negotiation logic and how to make such a negotiation process to be flexible but yet still efficient given that this process will most likely be executed many times.

3.4 Characteristics of Negotiation Standards

Based on the arguments that have been put so far, negotiation standards developed should consider the following:

- **Level of Negotiation**: negotiation standards should be developed as per the privacy level compliance as mentioned in section 2. The higher the negotiation level is, the better the privacy protection resulting from negotiation process is.
- **Balance of Power**: the amount and quality of information obtained during a negotiation process should be balanced, that is, "'I know about you just as much as you know about me"'. Quantifying how much information one gets might be challenging, but this is where standardization helps.

- **Accountability**: depending on the purpose of the negotiation, if accountability is important, then the information gained as a result from the negotiation process should be sufficient for a proper accountability process.
- **Negotiation Space**: negotiation standards should address the negotiation space. Section 3.3 provides an example of the possible negotiation space. Depending on the privacy level compliance, the more flexible the negotiation space is, the more likelihood that a negotiation will reach an agreement. A flexible negotiation standard should allow dynamic adjustment of the negotiation subjects so that all negotiating parties can reach an agreement.
- **Fail Over**: with proper negotiation level expectation and flexible negotiation space, a negotiation deadlock should hopefully be avoided. However, if it does happen, a negotiation standard should provide a method to solve this deadlock, such as the use of third party mediator. In the more extreme cases, service limitation or refusal might be the only solution, however, this should *only* occur due to unreasonable negotiation requirements from either or both parties.

The above negotiation characteristics are not meant to be exhaustive, but they represent some of the important issues to consider in developing negotiation standards.

4 Backward Privacy

While the use of privacy enhancing technologies represents developments in the right direction, it might be too late for people who are already active online. Chances are, a person's personal information have now been scattered, analyzed and profiled by myriads of organizations and consumer data aggregation companies such as Choicepoint [4] and Experian [5]. Experian, for example, even claimed that their database has compiled more than 98 percent of US household information [1].

As argued by Holtzman [4], the use of digital storage medium, and the increasingly cheaper data storage medium with gigantic storage capability, means that one can never be sure that a chunk of electronic data is ever deleted and disappeared. Copying and making backups of data are trivial tasks, unlike using paper as medium for information storage. The consequence of this is that, with an overwhelming probability, the personal information that has been revealed in the past is still retained. This is an issue that is especially important for those type of data that hardly change throughout one's life time, such as date of birth, tax file number, social security (or its equivalence outside US), and so forth. For such an information, while future transaction with privacy enhancing system could be as private as the user wants it to be, there is no protection for the usage of the revealed information in the past. We refer to this problem as backward privacy problem.

[4] http://www.choicepoint.net
[5] http://www.experiangroup.com/

Therefore, without efforts done to rectify this situation, the realistic expectations of having a privacy enhancing identity management system for today's users need to be re-assessed. This aspect of privacy has been overlooked most of the time, while we believe is an important part if one is serious about protecting users' privacy.

This issue has to be addressed from both the legal and technological perspectives. The legal aspect is beyond the scope of the paper. But at least from technological point of view, methods could be designed to provide ways to put this backward privacy issue into a manageable state. Or at the very least, there should be a standardized methods and guidelines in dealing with this problem.

The guidelines for the issue of backward privacy problem can also be done in-line with the privacy standards as mentioned in section 2. Depending on the level of privacy supported by a service provider, the compliance they have to deal with regard to backward privacy problem can be as simple as to do nothing with the existing data or, at the other end, to apply some technical solutions to allow a more manageable backward privacy.

By having a standardized guidelines on how to handle the backward privacy problem, combined with the use of privacy enhancing systems, the user thus knows what to expect of the treatment of their personal information that has already been released in the past so as to give a realistic expectation of the privacy level they have, even with the use of privacy enhancing identity management system in their future transactions.

4.1 Characteristics of Backward Privacy Standards

The following characteristics are not exhaustive, but it highlights several important areas that need to be addressed with regards to backward privacy. The term 'user information' in the following list refers to the personal information that has been revealed in the past to the service providers.

- **Archive Storage Period**: the time period that the user information will be stored in the archive after the introduction of the privacy enhancing identity system? This could vary, depending on the privacy level compliance, and the need of the archive for legal needs or business practicalities.
- **Security of the Archive**: the sort of security protection that will be applied to the archived users' information so that the use of privacy enhancing system is not compromised by the security breaches happening to the user information.
- **Nature of Treatment**: the treatments applied to the user information. Is the backward privacy treatment done in procedural manner that simply provides a set of guidelines that should be followed? Or, is the treatment is of more technical nature that might involve encryption or other technical security solutions?
- **Evidence**: the required evidence that a company should give to the users to confirm that the claimed treatment of the backward privacy problem has been implemented and preferably enforced.

– **Usage**: is the user information still usable? For example, can the user information still be shared, or used to provide services to users? Ideally this should not be allowed because those information that has been compromised can be re-used by identity theft to acquire services fraudulently.

Backward privacy is a problem that might face the most resistance to solve due to the involved cost for businesses. However, at the same time, it is a crucial issue to address if one is genuine in reclaiming the privacy that has been severely eroded.

5 Conclusion

This paper has put forward several potential areas for future standardization efforts in the identity management field. Most of the issues put forward here are those issues that would be greatly helped with the existence of standards. The importance of having privacy standards have been further argued, arguing from the users' usability perspective. Negotiation process is another area that needs standardization efforts because this capability could be abused, not to mention the potential deadlock situation in a negotiation process. Finally, the problem of backward privacy has been raised in this paper. While having a standard or guideline to tackle the issues mentioned in this paper is a crucial step, the enforcement to adopt these standards, once they are available, is another issue. The enforcement can be done from either the goodwill of the service providers to regain consumers trust, or through legal enforcement channel.

References

1. How do businesses use customer information:is the customers privacy protected? HEARING BEFORE THE SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION OF THE COMMITTEE ON ENERGY AND COMMERCE, HOUSE OF REPRESENTATIVES, July 2001. `http://republicans.energycommerce.house.gov/107/Hearings/07262001hearing336/hearing_print.htm`.
2. John Borking. Without privacy standards no trust. *1st PRIME Standardization Workshop on Standards for Privacy in User-Centric Identity Management*, 2006.
3. Marit Hansen, Henry Krasemann, et al. *PRIME (Privacy and Identity Management for Europe) - White Paper.* PRIME Consortium, July 2005.
4. David H. Holtzman. *Privacy Lost.* Jossey-Bass, 2006.
5. Audun Jøsang, Mohammed AlZomai, and Suriadi Suriadi. Usability and privacy in identity management architectures. *Proceedings of the Australasian Information Security Workshop (AISW) 2007*, January 2007.
6. Ronald Leenes, Simon Fischer-Hubner, et al. *PRIME (Privacy and Identity Management for Europe) - Framework V2.* PRIME Consortium, July 2006.
7. Dieter Sommer, Marc Wilikens, Walid Bagga, et al. *PRIME (Privacy and Identity Management for Europe) - Architecture V1.* PRIME Consortium, August 2005.
8. Adepele Williams and Ken Barker. Controlling inference: Avoiding p-level reduction during analysis. In *Conferences in Research and Practice in Information Technology (CRPIT) Vol 68*, 2007.